Algebra Universalis, 6 (1976) 269–275 Birkhäuser Verlag, Basel

A new proof of the congruence lattice representation theorem

PAVEL PUDLÁK

Introduction

The well known theorem, due to G. Grätzer and E. T. Schmidt [1] stating that every algebraic lattice is isomorphic to the congruence lattice of a (finitary) algebra, plays an important role in the universal algebra; it shows that there is no lattice-theoretical condition stronger than the condition of algebraicity satisfied by all congruence lattices. The original proof of this theorem was long and it used results about partial algebras. Some attempts were made to improve the proof in [2], [3], [4]. The proof presented here uses a different approach. Our way of producing an algebra (A, F) whose congruence lattice $\mathrm{Con}(A, F)$ is isomorphic with a given algebraic lattice can be intuitively described as follows:

(1) An algebraic lattice L is compactly generated, in fact, it is completely described by the set of all triples of compact elements α, α_1, α_2 such that $\alpha \leq \alpha_1 \vee \alpha_2$.

(2) A graph (A, r) with edges evaluated by compact elements of L can be constructed so that the unary algebra (A, F), whose operations are endomorphisms of (A, r) preserving the valuations in a certain sense, has its congruence lattice $\mathrm{Con}(A, F)$ isomorphic to L.

(3) Moreover, the graph (A, r) enables us to describe congruences $E \in \mathrm{Con}(A, F)$ through their intersections $E \cap r$.

(4) The required graph (A, r) has to satisfy several conditions of combinatorial character, which can be, more or less easily, fulfilled through an inductive construction from simpler graphs (cells) satisfying these conditions only partly.

I want to thank P. Goralčík, Z. Hedrlín, and J. Sichler who helped me to improve the proof.

I. Definitions

DEFINITION 1. Let K denote the set of all nonzero compact elements of a nontrivial algebraic lattice $\mathscr{L}$. A triple $\mathscr{A} = (A, r, h)$ is called a *K-valued graph* if

Presented by G. Grätzer. Received October 15, 1974. Accepted for publication in final form October 3, 1975.

(A, r) is an undirected graph without loops and $h: r \to K$ is a mapping of the set r of its edges into K.

If $\mathcal{A}_i = (A_i, r_i, h_i)$, $i = 0, 1$, are two K-valued graphs, a mapping $f: A_0 \to A_1$ is called *stable* if for every $\{a, b\} \in r_0$ either

$$f(a) = f(b)$$

or

$$\{f(a), f(b)\} \in r_1 \quad \text{and} \quad h_1(\{f(a), f(b)\}) = h_0(\{a, b\}).$$

Let Stab $(\mathcal{A})$ denote the monoid of all stable mappings of $\mathcal{A}$ into itself—the *stabilizer* of $\mathcal{A}$.

DEFINITION 2. Let F be a set of mappings of a set X into itself, let $\{a, b\}$, $\{c, d\}$ be subsets of X. Then $\{a, b\}$ *dominates* $\{c, d\}$ *through* F if there are $c = u_0, u_1, \ldots, u_n = d$ in X and $f_1, \ldots, f_n$ in F such that $\{f_i(a), f_i(b)\} = \{u_{i-1}, u_i\}$ for $i = 1, \ldots, n$; in notation, $\{a, b\}\ D_F\ \{c, d\}$.

If F is a monoid, then D_F is a transitive and reflexive relation.

NOTATION. For a given set X and a function f defined over the set X, denote by $P(X)$ the set of all subsets of X, by $Eq\ (X)$ the set of all equivalences on X, by f^+ the function defined over the set $P(X)$ by the formula

$$f^+(Y) = \{f(x) : x \in Y\} \quad \text{for} \quad Y \subseteq X.$$

DEFINITION 3. Let $\mathcal{A} = (A, r, h)$ be a K-valued graph, let $L \subseteq P(K)$ be the set of all ideals of the join-semilattice K. (L includes $\emptyset$). Let $\mathscr{C}$ denote the operator of the equivalence closure on A. Define two mappings $\varphi: L \to Eq\ (A)$, $\psi: \text{Con}\ (A, \text{Stab}\ (\mathcal{A})) \to P(K)$ by the formulas

$$\varphi(I) = \mathscr{C}h^{-1}(I), \quad \text{for} \quad I \in L,$$

$$\psi(E) = h^+(r \cap E), \quad \text{for} \quad E \in \text{Con}\ (A, \text{Stab}\ (\mathcal{A})).$$

In fact, $\varphi: L \to \text{Con}\ (A, \text{Stab}\ (\mathcal{A}))$, since every operation of the latter algebra is a stable mapping.

II

THEOREM. *Let* $\mathscr{A} = (A, r, h)$ *be a* K*-valued graph,* $F \subseteq \mathrm{Stab}(\mathscr{A})$ *and let us assume that*

(1) *h maps r onto K,*

(2) *if* $x \in r$ *and* $h(x) \leq \alpha_1 \vee \alpha_2$, $\alpha_1, \alpha_2 \in K$, *then there is a cycle* $x, x_1, \ldots, x_n$ *of* r *such that* $h(x_i) \in \{\alpha_1, \alpha_2\}$, *for* $i = 1, \ldots, n$,

(3) *if* $x, x_1, \ldots, x_n$ *is a cycle of* r, *then* $h(x) \leq h(x_1) \vee \cdots \vee h(x_n)$,

(4) *if* $x, y \in r$ *are such that* $h(x) = h(y)$, *then there is an* $f \in F$ *such that* $f^+(x) = y$,

(5) *if* $c \neq d$ *are in* A, *then there is a path* $x_1, \ldots, x_n \in r$ *connecting* c *to* d *such that* $\{c, d\} D_F x_i$ *for all* $i = 1, \ldots, n$.

Then $\psi(E) \in L$ for every congruence E of (A, F) and $\psi = \varphi^{-1}$.

Proof. (1) Let $\alpha_1, \alpha_2 \in \psi(E)$, $\alpha \leq \alpha_1 \vee \alpha_2$. Since h is onto, $\alpha = h(x)$ for some $x \in r$. By (2) there is a cycle $x, x_1, \ldots, x_n$ of r such that $h(x_i) \in \{\alpha_1, \alpha_2\}$, $i = 1, \ldots, n$. $\alpha_1 = h(y_1)$, $\alpha_2 = h(y_2)$ for some $y_1, y_2 \in r \cap E$, so that, by (4), every $x_i \in E$. Since $x, x_1, \ldots, x_n$ is a cycle, $x \in E$. Therefore $h(x) = \alpha \in \psi(E)$. Thus $\psi(E) \in L$.

(2) $\psi\varphi = 1$: Let I be an ideal of K. Since h is onto, $\psi\varphi(I) = h^+(r \cap \mathscr{C}h^{-1}(I)) \supseteq h^+h^{-1}(I) = I$. Conversely, if $x \in r \cap \mathscr{C}h^{-1}(I)$, then by (3), $\alpha = h(x) \leq h(x_1) \vee \cdots \vee h(x_n)$, where $x_1, \ldots, x_n \in h^{-1}(I)$ connect the endpoints of x. Since I is an ideal, $\alpha \in I$, which proves the opposite inclusion.

(3) $\varphi\psi = 1$: Let $E \in \mathrm{Con}(A, F)$, then $\varphi\psi(E) = \mathscr{C}h^{-1}h^+(r \cap E) \supseteq \mathscr{C}(r \cap E)$. Let $\{a, b\} \in \mathscr{C}h^{-1}h^+(r \cap E)$, then there is a path $x_1, \ldots, x_k \in r$ connecting a to b such that $h(x_i) = h(y_i)$ for some $y_i \in r \cap E$. (4) yields $x_i \in E$ so that $\{a, b\} \in \mathscr{C}(r \cap E)$. Since E is an equivalence, $E \supseteq \mathscr{C}(r \cap E)$. Now, let $\{c, d\} \in E$. (5) implies the existence of a path $z_1, \ldots, z_n$ of elements of r connecting c to d such that $\{c, d\} D_F z_i$, $i = 1, \ldots, n$. Since E is a congruence of (A, F), all z_i belong to E, so that $\{c, d\} \in \mathscr{C}(r \cap E)$. This finishes the proof.

III

Since φ and ψ are order-preserving mappings, L is isomorphic to the congruence lattice of (A, F). The remainder of the proof deals with the construction of a K-valued graph $\mathscr{A} = (A, r, h)$ which, together with its stabilizer $F = \mathrm{Stab}(\mathscr{A})$, satisfies (1)–(5) above.

DEFINITION 4. Let us construct a K-valued graph $\mathscr{B}_\alpha = (B_\alpha, s_\alpha, k_\alpha)$ for every $\alpha \in K$, ($\mathscr{B}_\alpha$ will be called the *α-cell*) as follows: set $\alpha C = \{\langle \alpha_1, \alpha_2 \rangle : \alpha \leq \alpha_1 \vee \alpha_2\}$. For every $\mathbf{a} = \langle \alpha_1, \alpha_2 \rangle \in \alpha C$ denote

(+) $x_i^{\mathbf{a}} = \{u_{i-1}^{\mathbf{a}}, u_i^{\mathbf{a}}\}$,

$i = 1, 2, 3, 4$, where $u_0^{\mathbf{a}} = a$, $u_4^{\mathbf{a}} = b$, for all $\mathbf{a} \in \alpha C$, and all the other points are distinct.

Set

$$B_\alpha = \{a, b\} \cup \{u_i^{\mathbf{a}} : i = 1, 2, 3, \mathbf{a} \in \alpha C\},$$

$$s_\alpha = \{\{a, b\}\} \cup \{x_i^{\mathbf{a}} : i = 1, 2, 3, 4, \mathbf{a} \in \alpha C\},$$

$$k_\alpha(\{a, b\}) = \alpha,\ k_\alpha(x_1^{\mathbf{a}}) = k_\alpha(x_3^{\mathbf{a}}) = \alpha_1,\ k_\alpha(x_2^{\mathbf{a}}) = k_\alpha(x_4^{\mathbf{a}}) = \alpha_2.$$

$\{a, b\}$ will be called the *base* of the α-cell $\mathcal{B}_\alpha$. (+) is called a *chain* of $\mathcal{B}_\alpha$. In the sequel the superscripts are omitted.

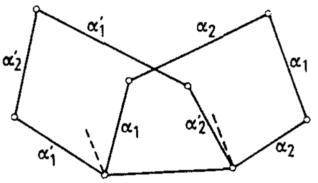

Figure 1

The required K-valued graph $\mathcal{A} = (A, r, h)$ is constructed by induction as follows.

Choose an element α_0 of K. $\mathcal{A}_0$ will be a single edge valued by α_0. If $\mathcal{A}_n = (A_n, r_n, h_n)$ had already been constructed, produce $\mathcal{A}_{n+1}$ as follows:

Let $x \in r_n - r_{n-1}$, $x = \{c, d\}$, $h_n(x) = \alpha$. Attach a copy of $\mathcal{B}_\alpha$ to $\mathcal{A}_n$, identifying $\{c, d\}$ with the base $\{a, b\}$ of $\mathcal{B}_\alpha$, arbitrarily by the identification $a = c$, $b = d$ or $a = d$, $b = c$. In other words, the extended graph has the set of vertices $A_n \cup (B_\alpha - \{a, b\})$, and $r_n \cup (s_\alpha - \{\{a, b\}\})$ are all its edges. Since $h_n(x) = \alpha = k_\alpha(\{a, b\})$, the common extension of h_n and k_α is well-defined. Applying this one step extension to every $x \in r_n - r_{n-1}$ we arrive at $\mathcal{A}_{n+1} = (A_{n+1}, r_{n+1}, h_{n+1})$.

Note that $A_n \subseteq A_{n+1}$, $r_n \subseteq r_{n+1}$, $h_n \subseteq h_{n+1}$, so that we may define $\mathcal{A} = (A, r, h)$ by

$$A = \bigcup_{n=0}^{\infty} A_n, \qquad r = \bigcup_{n=0}^{\infty} r_n, \qquad h = \bigcup_{n=0}^{\infty} h_n,$$

and that $\mathcal{A}$ indeed is a K-valued graph.

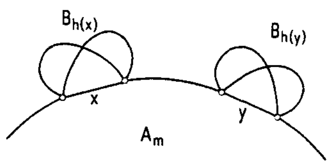

Figure 2

CLAIM 1. $\mathcal{A}$ satisfies (1), (2), (3).

Proof. (1) Since $\alpha_0 \leq \alpha_0 \vee \alpha$ for all $\alpha \in K$, h_1 is already an onto mapping.

(2) Every edge $x \in r$ is the base of a copy of an $h(x)$-cell. Thus if $h(x) \leq \alpha_1 \vee \alpha_2$, then the cycle $x, x_1, \ldots, x_4$ valued by $\alpha, \alpha_1, \alpha_2, \alpha_1, \alpha_2$ has been included in $\mathcal{B}_{h(x)}$.

(3) is true for $\mathcal{A}_0$, since it contains no cycles. If proved for all cycles in $\mathcal{A}_m$, assume that $x, x_1, \ldots, x_n$ is a cycle in $\mathcal{A}_{m+1}$. If $x \in r_{m+1} - r_m$, then x lies on one of the chains of some $\mathcal{B}_\alpha$ added at the $(m+1)$-st step and every cycle containing x has to contain this whole chain—which contains another edge y with $h(x) = h(y)$. Thus $h(x) = h(x_k)$ for some k and $h(x) \leq \bigvee_{i=1}^{n} h(x_i)$. If $x \in r_m$, then by replacing every portion of the cycle $x, x_1, \ldots, x_n$ not contained in r_m by the base of its cell we obtain a cycle $x, y_1, \ldots, y_k$ in r_m satisfying $h(x) \leq \bigvee h(y_i) \leq \bigvee h(x_i)$, by induction hypothesis and by an easy observation that the value of the base of an arbitrary α-cell is majorized by the join of evaluations of the edges of any of its chains.

The conditions (4) and (5) involve the stabilizer of $\mathcal{A}$—they say that "there are enough stable mappings". To prove these two conditions, we will define certain stable mappings explicitly.

First of all, note that there is a stable involution of every cell $\mathcal{B}_\alpha$ onto itself which interchanges the endpoints of the base of $\mathcal{B}_\alpha(\langle \alpha_1, \alpha_2 \rangle \in \alpha C$ iff $\langle \alpha_2, \alpha_1 \rangle \in \alpha C)$. This gives rise to the following:

CLAIM 2. Every stable mapping $f: \mathcal{A}_n \to \mathcal{A}_m$ can be extended to a stable mapping $f': \mathcal{A}_{n+1} \to \mathcal{A}_{m+1}$ and, consequently, to a stable mapping $f'': \mathcal{A} \to \mathcal{A}$.

Proof. If $t \in A_{n+1} - A_n$, denote by $\{a, b\}$ the base of a cell $\mathcal{B}$ containing t. If $f(a) = f(b)$, set $f'(t) = f(a)$. If $c = f(a) \neq f(b) = d$, then $h_n(\{a, b\}) = h_m(\{c, d\})$ since f is stable. Therefore $\{c, d\}$ is the base of another copy of the cell $\mathcal{B}$. f' is the extension of f by the bijection of $\mathcal{B}$ which is determined by $f|_{\{a,b\}}$. In both cases it is clear that f' is again stable.

DEFINITION 5. Let $x \in r_m - r_{m-1}$, $m > 0$. Define $f_x: \mathcal{A}_m \to \mathcal{A}_m$ as follows: $x = x_k$ in some chain x_1, x_2, x_3, x_4 of a cell based on $\{a, b\} \in r_{m-1}$, $a = u_0$, $b = u_4$, $x_i = \{u_{i-1}, u_i\}$, $h_m(x_j) = h_m(x_{j+2}) = \alpha_j$ for $j = 1, 2$.

If $k = 1, 2$, set

$$f_{x_k}(u_k) = f_{x_k}(u_{k+1}) = u_k,$$

$$f_{x_k}(y) = u_{k-1} \quad \text{for all other} \quad y \in A_m,$$

if $k=3, 4$ set

$$f_{x_k}(u_k)=f_{x_k}(u_{k-1})=u_{k-1},$$

$$f_{x_k}(y)=u_k \quad \text{for all other} \quad y\in A_m.$$

For $x\in r_0$ let f_x be the identity mapping on A_0. In particular, $f^+_{x_k}(A_m)=x_k$, all f_{x_k} are stable.

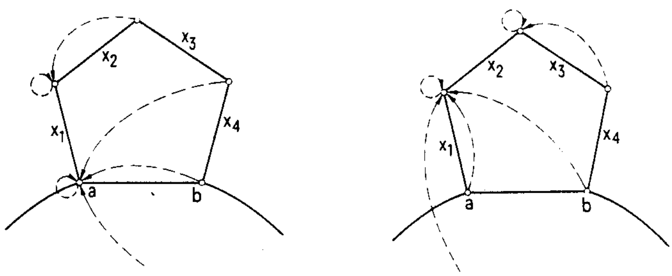

Figure 3

CLAIM 3. $\mathscr{A}$ satisfies (4).

Proof. Let $x\in r_m-r_{m-1}$, $y\in r_n$, $h(x)=h(y)$. Let $f_x:\mathscr{A}_m\to\mathscr{A}_m$ be the stable mapping defined above. Since $f^+_x(A_m)=x$, the composite mapping $g\circ f_x$—where $g:x\to y$ is a bijection—is also a stable mapping of $\mathscr{A}_m\to\mathscr{A}_n$. By Claim 2., $g\circ f_x$ can be extended to a stable $f:\mathscr{A}\to\mathscr{A}$.

CLAIM 4. $\mathscr{A}$ satisfies (5).

Proof. By induction: Since the identity mapping of A is in F, all the edges of r satisfy (5), in particular $\mathscr{A}_0$ satisfies (5).

The induction step $\mathscr{A}_m\to\mathscr{A}_{m+1}$: Let c, $c'\in A_{m+1}$, $\{c, c'\}\notin r$, $c\neq c'$. We shall construct a path $x_1,\dots,x_s$ connecting some point a in A_m to c. When $c\in A_m$, the path is empty. If $c\in A_{m+1}-A_m$, then c lies on some chain $a=u_0,\dots,u_4=b$ of a cell with base $\{a, b\}$, joined in the $m+1$-th step, say $c=u_s$, $0<s\leq 2$. Then the path $x_1,\dots,x_s$ is $\{u_0, u_1\},\dots,\{u_{s-1}, u_s\}$. Since $\{c, c'\}\notin r$, we have $c'\neq u_{s+1}$, $c'\neq u_{s-1}$, therefore f_{x_i} maps $\{c, c'\}$ onto x_i for $i=1,\dots,s$. Thus $\{c, c'\}$ dominates $\{c, a\}$. Similarly, there is a path $x'_1,\dots,x'_t$ connecting some point a' in A_m to c' such that $\{c, c'\}D_Fx'_1,\dots,x'_t$, consequently $\{c, c'\}D_F\{c', a'\}$. Since, clearly, $\{c, c'\}D_F\{c, c'\}$ through identical mapping, we have $\{c, c'\}D_F\{a, a'\}$. Now, by induction hypothesis, there is a path in r connecting a to a', say $y_1,\dots,y_n$, such that $\{a, a'\}D_Fy_i$ for all $i=1,\dots,n$. Since F is a monoid, D_F is transitive so that $\{c, c'\}D_Fy_1,\dots,y_n$. Hence $x_s,\dots,x_1, y_1,\dots,y_n, x'_1,\dots,x'_t$ is the desired path in r connecting c to c'.

REFERENCES

[1] G. GRÄTZER and E. T. SCHMIDT, *Characterization of congruence lattices of abstract algebra.* Acta Sci. Math. Szeged *24* (1963), 34–59.
[2] G. GRÄTZER, *Universal Algebra.* D. Van Nostrand Co., 1968.
[3] B. JÓNSSON, *Topics in Universal Algebra.* Lecture notes, Vanderbilt University, 1969–70.
[4] E. T. SCHMIDT, *Kongruenzrelationen algebraischer Strukturen.* Math. Forschungsberichte, *25* (1969).

Charles University
Praha
Czechoslovakia